REMARKS

Claims 1 – 31 are pending in the application. Claims 1, 13, 14, and 21 are currently amended.

Claim Rejections – 35 USC 103

Claims 1 – 8, 13 – 16, and 21 - 27 were rejected under 35 USC 103(a) as being unpatentable over the article by Jung, in view of Shefi US 6,266,413.

The Examiner further rejected claims 9-12,17-20, and 28-31 under 35 USC 103(a) as being unpatentable over Jung and Shefi, in further view of Midgley et al, US Patent No. 6,460,055.

Favorable reconsideration of this rejection in view of the above amendments and the following explanations is respectfully requested.

The present invention, as described in the Field of the Invention section, relates to a method and an apparatus for the provision of random data, and more particularly but not exclusively to a practical method and apparatus for providing identical random data in a confidential manner to parties connected via an open network.

The present invention teaches a novel and inventive method for providing identical genuine random data at two or more separate locations. The random data has a single source, which *is external* to the two parties and may be accessible to anyone. Nevertheless, the method provides confidentially to each of the locations in such a way that it is not available to eavesdroppers, using an identical selector deployed at each of the parties. Each of the identical selectors selects the *same* random bit source from the single external source, at the respective party.

The Shefi system provides a totally opposite solution. With the Shefi system, two parties share a *secret source* – a large table of random number (or several such tables). To start a process between the two parties they send to each other a starting pointer. The starting pointer is sent in the *open, not in secret.* The pointer is then used to move along the same secret table at both parties. That is to say, the pointer starting tuning is not secret, and a third party can also have the pointer starting tuning. The secrecy is supposed to be achieved by the secrecy of the *secret source* large table of random number that both parties have and no third party has.

Jung describes a CFB-mode of encryption. The CFB-mode of encryption is well known and has been used for long time, for many decades, and is written and explained in almost any basic textbook of cryptography.

With the CFB-mode, the ciphertext is copied in *serial order of appearance* as a whole into the register, generally byte by byte, and the register is shifted. The output of the register is processed serially using a secret key by a block cipher algorithm to output a stream of bits for XOR-ing the stream with the plaintext. With Jung, the only secret element is the secret key and no selection whatsoever occurs.

Claim 1, as currently amended, defines a system for sharing a random process between at least two separate parties, the system comprising at each party: a copy of a part of a primary digital bitstream, the primary digital stream being *located externally* to the at least two separate parties, the copy being available at respective ones of the separate parties, and a selector for randomly selecting the part of the primary digital bitstream to form a random bit source, wherein each selector is operable to use the random bit source to randomize the selection operation in an identical manner at each

separate party, thereby to render the random bit source available at respective ones of the separate parties.

The present invention, as defined by claim 1, teaches a system which uses a copy of an *external* primary digital bitstream, and includes a selector for randomly selecting parts of the copy of the *external* primary digital bitstream to form a random bit source. That is to say, with the present invention, the random data has a single source, which *is external* to the two parties, and is typically accessible to anyone.

For example, the present invention describes on page 21, line 7: "Thus, the processes described above may rely on any source of highly shuffled data including external sources, and do not require any initial arrangement of the data in order to use the data in real time operation".

By contrast, the Shefi system provides a totally opposite solution. With the Shefi system, two parties share a *secret source* – a large table of random number (or several such tables). That is to say, with Shefi, the primary digital bitstream is secret and internal to the participating parties only, whereas a starting pointer used for pointing at starting position at the secret table and generating a random bit stream may be open to the public as is sent from the parties to each other in the open.

For example, Shefi describes in column 10, line 22: "The system includes an electronic device, for example a semiconductor chip, which contains at least one table of random numbers, and which is able to generate an electronic "one-time pad". In order for secure communication to take place, each party must have this chip or another form of the electronic device of the present invention. Any two parties having the electronic device of the present invention can then communicate securely or perform a secure identification procedure."

Shefi further describes in column 10, line 30: "In either case, the two parties preferably send at least one random number to each other as part of the key. The key is then used as part of the method of the present invention for generating an electronic "one-time pad" by selecting at least one true random number from a table of true random numbers according to a selection procedure."

However, Shefi never describes or even hints at the idea of a system using an *external* primary digital bitstream, nor a randomly changed totally secret selection as taught by the present invention, and defined by claim 1.

As described hereinabove, Jung also fails to describe or even hint at the idea of a system using an *external* primary digital bitstream, with a randomly changed secret selection as taught by the present invention, and defined by claim 1. With Jung, the *only secret element is the secret key* and *no (secret) selection* whatsoever occurs.

For example, Jung describes on page 344, in section 3.1: "In a standard case, n bits of the ciphertext are fed back into the shift register, i.e. if n bits of generated key steam are used for the encryption of n bits of plaintext."

Thus Shefi combined with Jung also fails short of teaching the idea of a system using an *external* primary digital bitstream, nor a randomly changed secret selection as taught by the present invention, and defined by claim 1.

It is thus respectfully believed that claim 1 as amended is novel and inventive over both Jung and Shefi and should be allowed.

Claim 13, as currently amended, defines a random data generator comprising: an input means for receiving a copy of a part of a digital bitstream, the digital bit stream being *located externally* to parties using the generator, a random selector for selecting

random individual bits from the digital bitstream to form the part, the part comprising a random data stream, wherein the random selector is randomized by a previous segment of the random data stream, such as to allow the random data stream to be available at any location at which the part of the digital bitstream is available.

The present invention, as defined by claim 13 and explained hereinabove, teaches a random data generator which uses a copy of an *external* digital bitstream, and includes a random selector for randomly selecting parts of the copy of the *external* digital bitstream to form a random bit source.

That is to say, with the present invention, the random data has a single source, which *is external* to the two parties, and an inherent randomly changed random secret selector.

As explained in further detail hereinabove, neither Jung nor Shefi teaches or even hints at the idea of a random data generator using a copy of an *external* digital bitstream, nor an inherent randomly changed random secret selector as taught by the present invention, and defined by claim 13.

It is thus respectfully believed that claim 13 as amended is novel and inventive over both Jung and Shefi and should be allowed.

Claim 14, as currently amended, defines a random data generator for reproducing a random data stream producible by an identical generator at another location, comprising: an input means for receiving a copy of a part of a digital bitstream, the copy of the part of the digital bitstream being available in identical manner at a plurality of locations, the digital bit stream being *external* to the locations, a random selector for selecting the part, the part comprising random individual bits from the bitstream, therefrom to form a random data stream, wherein the random selector is

randomized by a previous segment of the random data stream, thereby to enable the random data stream to be available in identical manner at a plurality of locations.

The present invention, as defined by claim 14 and explained hereinabove, teaches a random data generator which uses a copy of an *external* digital bitstream, and includes a random selector for randomly selecting parts of the copy of the *external* digital bitstream to form a random bit source.

That is to say, with the present invention, the random data has a single source, which *is external* to the two parties and an inherent randomly changed random secret selector.

As explained in further detail hereinabove, neither Jung nor Shefi teaches or even hints at the idea of a random data generator using a copy of an *external* digital bitstream, nor an inherent randomly changed random secret selector as taught by the present invention, and defined by claim 14.

Claim 21, as currently amended, defines a method for sharing a random process between at least two separate parties, comprising the steps of: randomly selecting at each party a copy of a part of a primary digital data bit stream, the primary digital data bit stream being *external* to the parties and available in identical manner at each party, the copy to form a random data source, and using the random data source to randomize the selection operation in an identical manner at each party, thereby to render the random process available in identical manner at each party.

That is to say, with the present invention, the random data has a single source, which *is external* to the two parties and an inherent randomly changed random secret selector.

As explained in further detail hereinabove, neither Jung nor Shefi teaches or even hints at the idea of a method using a copy of an *external* digital bitstream, nor an inherent randomly changed random secret selector as taught by the present invention, and defined by claim 21.

The remaining claims mentioned in this section of the Office Action are believed to be allowable as being dependent on an allowable main claim.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable.

An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan
Registration No. 40,338

Date: September 7, 2006

Encl.:
Petition for Extension of Time (3 Months)